REMARKS

In an Office Action dated July 3, 2007, the Examiner has rejected Claims 1-5, 7-13 and 16 under 35 USC § 103(a) as being unpatentable over USPN 7,142,676 issued to Hillier et al. ("Hillier") in view of USPN 6,336,121 issued to Lyson et al. ("Lyson") and further in view of USPN 6,256,733 issued to Thakkar et al. ("Thakkar"). The Examiner has rejected Claims 6, 14-15, 17 and 20 under 35 USC § 103(a) as being unpatentable over Hillier in view of Lyson and further in view of US Pub. No. 2003/0194093 issued to Evans et al. ("Evans"). The Examiner has rejected Claims 18-19 and 21 under 35 USC § 103(a) as being unpatentable over Hillier in view of Lyson and further in view of Thakkar and still further in view of Evans.

In this response, Applicant respectfully traverses the rejection of Claims 1-21. Applicant requests reconsideration of in view of arguments as set forth in detail in the following remarks.

CLAIM REJECTIONS – 35 U.S.C. § 103

With reference to the independent claims 1, 10 and 18, the Examiner has rejected Claims 1 and 10 for identical reasons, arguing that the claims are unpatentable over Hillier in view of Lyson, and further in view of Thakkar. The Examiner has similarly rejected Claim 18, arguing that the claims are unpatentable over Hillier in view of Lyson, further in view of Thakkar, and further in view of Evans. Applicant traverses the rejections of Claims 1, 10, and 18 for the following reasons.

Hillier discloses the use of a third party processor to facilitate decryption. A recipient of encrypted information from an originator is required to use the third party processor to obtain a decryption key so that the delivery of the encrypted information to

the recipient can be confirmed. The Examiner argues that Hillier discloses the generating

and decrypting elements of Claim 1 and 10, namely the first and second entities

generating and encrypting keys using the public key of a third entity, as well the third

entity decrypting those keys using its private key. Applicant disagrees. At best, Hillier

arguably discloses the encryption of a security token by an originator using a public key

associated with the third party, where the originator is arguably analogous to the second

entity/application recited in Claim 1. However, nothing in Hillier discloses a recipient

generating and encrypting a key with the public key of the third entity, much less the

third entity encrypting the recipient's key with the originator's key, and the originator

obtaining and decrypting the encrypted recipient's key with the originator's key. If

anything, Hillier indicates that the third party is not capable of encrypting, but rather only

capable of partially decrypting a double key package received from a recipient in order to

recover a decryption key on behalf of the recipient.

     The Examiner concedes that Hillier fails to disclose a third entity encrypting the

first key using the second key and a second entity obtaining the first key encrypted by the

second key and decrypting the first key using the second key. But the Examiner argues

that Lyson discloses the re-encrypting of a temporarily decrypted symmetric key after

providing decrypted data to a requestor as shown in FIG. 3 of Lyson, and concludes that

it would have been obvious to combine Hillier with Lyson in order to have a reduced

number of keys. Applicant disagrees. Lyson discloses securing data in a database by

encrypting a symmetric key using a requester's public key. The key is temporarily

decrypted upon receiving a request for data from the database, and then re-encrypted

again using the requester's public key after the data has been provided to the requester.

Nothing in Lyson teaches or suggests a third entity encrypting a first key using a second key where the first key is the recipient's key and the second key is the originator's key, much less the originator obtaining and decrypting the encrypted recipient's key with the originator's key. Moreover, Applicant fails to see how a reduced number of keys provides the motivation to combine Lyson and Hillier.

The Examiner further concedes that neither Hillier nor Lyson disclose the encrypting of keys using the public key of an entity. But the Examiner argues that Thakkar discloses the encrypting of keys using a public key, and concludes that it would have been obvious to combine Thakkar with Hillier and Lyson to provide for signature verification using publicly available data. Applicant disagrees. Thakkar merely discloses a conventional use of a public/private key pair to provide signature verification for the sending and receiving parties and does not disclose a secure key exchange between the parties.

With reference to independent Claim 18, the Examiner concedes that neither Hillier, Lyson, not Tahakkar disclose pseudo-randomly generated keys. But the Examiner argues that Evans discloses a pseudo-randomly generated key, and concludes that it would have been obvious to combine Hiller, Lyson, Thakkar and Evans, to have a key that is never revealed. The Examiner further concedes that Hillier, Lyson, not Tahakkar disclose registers for storing keys or an input/output pin dedicated to use by a first entity. But the Examiner argues that Evans also discloses such registers and pins, and that it would have been obvious to combine the teachings of the references to have a unit for storing keys. Applicant disagrees. Even if Evans cures the aforementioned deficiencies of Hillier, Lyson and Thakkar, none of those references disclose the first,

second, and third entities as recited in the independent claims as the Applicant has

submitted above. Moreover, among other deficiencies, none of the prior art of record

discloses a trusted platform module (TPM) as described in the specification and recited in

Claim 18 and its dependent claims.

  In view of the foregoing, Applicant submits that independent claims 1, 10 and 18

are patentably distinguishable over the cited art of record, either alone or in combination.

Dependent claims 2-9, 11-17, and 19-21 are allowable because they depend from

allowable independent claims 1, 10 and 18, and because of their additional limitations.

Consequently, reconsideration and allowance of Claims 1-21 is respectfully requested.

CONCLUSION

For at least the foregoing reasons, Applicant submits that the rejections have been overcome. Therefore, claims 1-21 are in condition for allowance and such action is earnestly solicited. The Examiner is respectfully requested to contact the undersigned by telephone if such contact would further the examination of the present application. Please charge any shortages and credit any overcharges to our Deposit Account number 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: <u>November 5, 2007</u>   <u>/Donna Jo Coningsby/</u>
                                       Donna Jo Coningsby
                                       Reg. No. 41,684
                                       Attorney for Applicant(s)

                                       1279 Oakmead Parkway
                                       Sunnyvale, CA 94085-4040
                                       (503) 439-8778